R7-44 System Access - Secure Logoff Procedures

NPAC SMS shall provide a mechanism to end the session through secure logoff procedures.

R7-45

(Duplicate - refer to R7-47)

R7-46 System Access, Unauthorized Use Message - Specifiable

NPAC SMS shall ensure that the message is NPAC SMS-specifiable to meet their own requirements, and any applicable laws.

R7-47.1 System Access, Unauthorized Use Message - Specifiable

NPAC SMS shall be able to display an advisory warning message of up to 20 lines in length prior to login.

R7-47.2 Advisory Warning Message Default

NPAC SMS shall default the pre-login advisory warning message to the following:

NOTICE: This is a private computer system.
Unauthorized access or use may lead to prosecution.

R7-48.1 System Access - User's Last Successful Access

NPAC SMS shall display the date and time of the user's last successful system access upon successful login.

R7-48.2 System Access - User's Unsuccessful Access Attempts

NPAC SMS shall display the number of unsuccessful attempts by that userId to access the system, since the last successful access by that userId upon successful login.

R7-49.1 System Access, Security Administration - Authorize Users

NPAC SMS shall only allow the NPAC Security Administrator to authorize users.

R7-49.2 System Access, Security Administration - Revoke Users

NPAC SMS shall only allow the NPAC Security Administrator to revoke users.

R7-50.1 System Access, Security Administration -Adding Users

NPAC SMS shall provide security documentation that defines and describes procedures for adding users.

R7-50.2 System Access, Security Administration -Deleting Users

NPAC SMS shall provide security documentation that defines and describes procedures for deleting users.

7.4.2 Resource Access

R7-51 Data Access for Authorized Users

NPAC SMS shall allow only authorized users to access the data that is part of or controlled by the SMS system.

R7-52 Service Provider Data Protected

NPAC SMS shall protect service provider data from access by unauthorized users.

R7-53.1 Authorized User Access to Software

NPAC SMS shall ensure that only NPAC system administrators can access the software files that constitutes the NPAC SMS.

R7-53.2 Authorized User Access to Transactions

NPAC SMS shall ensure that only authorized users can access the transactions that constitute the NPAC SMS.

R7-53.3 Authorized User Access to Data

NPAC SMS shall ensure that only authorized NPAC Administrative and NPAC SOA Low-tech Interfaces users can access the data generated by the transactions that constitutes the SMS.

R7-54.1 Access Control of Executable Software

NPAC SMS shall ensure that the executable and loadable software is access controlled for overwrite and update, as well as execution rights.

R7-55 Access Control of Resources

NPAC SMS shall ensure that control of access to resources is based on authenticated user identification.

R7-56 Use of Encryption

NPAC SMS shall ensure that userId and password is used as a primary access control for direct login and system ID is used for primary access control to the SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface.

R7-57 Resource Access to Users

NPAC SMS shall ensure that for software resources controlled by NPAC SMS, it must be possible to grant access rights to a single user or a group of users.

R7-58 Resource Access Denied to Users

NPAC SMS shall ensure that for software resources controlled by NPAC SMS, it must be possible to deny access rights to a single user or a group of users.

R7-59

(Duplicate - refer to R7-53.3)

R7-60 Only NPAC Personnel Can Modify User Access

NPAC SMS shall allow only NPAC personnel to modify access rights to a resource.

R7-61 Removal of User Access Rights

NPAC SMS shall provide a mechanism to remove access rights to all software resources for a user or a group of users.

R7-62.1

(Duplicate - refer to R7-12)

R7-62.2

(Duplicate - refer to R7-12)

7.5 Data and System Integrity

R7-63 Identify Originator of System Resources

NPAC SMS shall identify the originator of any accessible system resources.

R7-64 Identify Originator of Information Received Across Communication Channels

NPAC SMS shall be able to identify the originator of any information received across communication channels.

R7-65.1 Monitor System Resources

NPAC SMS NMS shall use SNMP to monitor the system resources.

R7-65.2 Detect Error Conditions

NPAC SMS NMS shall use SNMP to detect error conditions.

R7-65.3 Detect Communication Errors

NPAC SMS NMS shall use SNMP to detect communication errors.

R7-65.4 Detect Link Outages

NPAC SMS NMS shall use SNMP to detect link outages.

R7-66.1 Rule Checking on Update

NPAC SMS shall ensure proper rule checking on data update.

R7-66.2 Handling of Duplicate Inputs

NPAC SMS shall handle duplicate/multiple inputs.

R7-66.3 Check Return Status

NPAC SMS shall check return status.

R7-66.4 Validate Inputs

NPAC SMS shall validate inputs for reasonable values.

R7-66.5 Transaction Serialization

NPAC SMS shall ensure proper serialization of update transactions.

R7-67 Database Integrity Checking

NPAC SMS shall include database integrity checking utilities for the NPAC SMS database.

7.6 Audit

7.6.1 Audit Log Generation

R7-68.1 Security Audit Log for After the Fact Investigation

NPAC SMS shall generate a security audit log that contains information sufficient for after the fact investigation of loss or impropriety for appropriate response, including pursuit of legal remedies.

R7-68.2 Security Audit Data Availability

NPAC SMS shall ensure that the security audit data is available on-line for a minimum of 90 days.

R7-68.3 Security Audit Data Archived

NPAC SMS shall archive the security audit data off-line for a minimum of two years.

R7-69 User Identification Retained

NPAC SMS shall ensure that the user-identification associated with any NPAC SMS request or activity is maintained, so that the initiating user can be traceable.

R7-70 Protection of Security Audit Log Access

NPAC SMS shall protect the security audit log from unauthorized access.

R7-71.1

DELETE

R7-71.2 NPAC Personnel Delete Security Audit Log

NPAC SMS shall ensure that only authorized NPAC personnel can archive and delete any or all of the security audit log(s) as part of the archival process.

R7-72 Security Audit Control Protected

NPAC SMS shall ensure that the security audit control mechanisms are protected from unauthorized access.

R7-73.1 Log Invalid User Authentication Attempts

NPAC SMS shall write a record to the security audit log for each invalid user authentication attempt.

R7-73.2 Log NPAC SMS End User Logins

NPAC SMS shall write a record to the security audit log for logins of NPAC users.

R7-73.3 Log NPAC Personnel Activities

NPAC SMS shall write a record to the security audit log for security controlled activities of NPAC users.

R7-73.4 Log Unauthorized Data Access

NPAC SMS shall write a record to the security audit log for unauthorized data access attempts.

R7-73.5 Log Unauthorized Transaction Access

NPAC SMS shall write a record to the security audit log for unauthorized NPAC SMS transaction functionality access attempts.

R7-74 No Disable of Security Auditing

NPAC SMS shall ensure that NPAC audit capability cannot be disabled.

R7-75 Security Audit Record Contents

NPAC SMS shall ensure that for each recorded event, the audit log contains the following:

- Date and time of the event
- User identification including relevant connection information
- Type of event
- Name of resources accessed or function performed
- Success or failure of the event

R7-76.1 Recorded Login Attempts

NPAC SMS shall record actual or attempted logins in audit logs after an NPAC-tunable parameter threshold of consecutive login failures.

7.6.2 Reporting and Intrusion Detection

R7-77.1 Exception Reports on Data Items

NPAC SMS shall provide post-collection audit analysis tools that can produce exception reports on items relating to system intrusions.

R7-77.2 Exception Reports on Users

NPAC SMS shall provide post-collection audit analysis tools that can produce exception reports on users relating to system intrusions.

R7-77.3 Exception Reports on Communication Failures

NPAC SMS shall provide post-collection audit analysis tools that can produce exception reports on communication failures relating to system intrusions.

R7-77.4 Summary Reports on Data Items

NPAC SMS shall provide post-collection audit analysis tools that can produce summary reports on data items relating to system intrusions.

R7-77.5 Summary Reports on Users

NPAC SMS shall provide post-collection audit analysis tools that can produce summary reports on users relating to system intrusions.

R7-77.6 Summary Reports on Communication Failures

NPAC SMS shall provide post-collection audit analysis tools that can produce summary reports on communication failures relating to system intrusions.

R7-77.7 Detailed Reports on Data Items

NPAC SMS shall provide post-collection audit analysis tools that can produce detailed reports on data items relating to system intrusions.

R7-77.8 Detailed Reports on Users

NPAC SMS shall provide post-collection audit analysis tools that can produce detailed reports on users relating to system intrusions.

R7-77.9 Detailed Reports on Communication Failures

NPAC SMS shall provide post-collection audit analysis tools that can produce detailed reports on communication failures relating to system intrusions.

R7-78 Review User Actions

NPAC SMS shall provide a capability to review a summary of the actions of any one or more users, including other NPAC users, based on individual user identity.

R7-79.1 Monitor Network Address

NPAC SMS shall provide tools for the NPAC to monitor the message passing activities to and from a specific network address as they occur.

R7-80.1 Real-time Security Monitor

NPAC SMS NMS shall provide a real-time mechanism to monitor the occurrence or accumulation of security auditable events. Where possible, NPAC SMS shall determine and execute the least disruptive action to terminate the event.

R7-80.2 Security Event Notification

NPAC SMS NMS shall notify the NPAC personnel immediately when security event thresholds are exceeded through the SNMP agent.

7.7 Continuity of Service

R7-81 System Made Unavailable by Service Provider

NPAC SMS shall ensure that no service provider action, either deliberate or accidental, should cause the system to be unavailable to other users.

R7-82 Detect Service Degrading Conditions

NPAC SMS shall report conditions that would degrade service below a pre-specified minimum, including high memory, CPU, network traffic, and disk space utilization.

R7-83 System Recovery After Failure

NPAC SMS shall provide procedures or mechanisms to allow recovery after a system failure without a security compromise.

R7-84.1 Software Backup Procedures

NPAC SMS shall have documented procedures for software backup.

R7-84.2 Data Backup Procedures

NPAC SMS shall have documented procedures for data backup.

R7-84.3 Software Restoration Procedures

NPAC SMS shall have documented procedures for software restoration.

R7-84.4 Data Restoration Procedures

NPAC SMS shall have documented procedures for data restoration.

R7-85.1 Software Version Number

NPAC SMS shall record the exact revision number of the latest software installed.

R7-85.2 Software Version Number

NPAC SMS shall display for viewing the exact revision number of the latest software via a Web bulletin board, and also through the NPA Administrative and NPAC SOA Low-tech Interfaces upon completion of the user login sequence.

7.8 Software Vendor

R7-86 Software Development Methodology

NPAC SMS shall be developed using a corporate policy governing the development of software.

R7-87 Bypass of Security

NPAC SMS shall **not** support any mode of entry into NPAC SMS for maintenance, support, or operations that would violate or bypass any security procedures.

R7-88 Documented Entry

NPAC SMS shall document any mode of entry into the SMS for maintenance, support, or operations.

7.9 OSI Security Environment

7.9.1 Threats

Attacks against the NPAC SMS may be perpetrated in order to achieve any of the following:

- Denial of service to a customer by placing wrong translation information in the SMS
- Denial of service to a customer by preventing a valid message from reaching the SMS
- Disrupting a carrier's operations by having numerous spurious calls (to users who are not clients of that carrier) directed to that carrier
- Switching customers to various carriers without their consent
- Disrupting the functioning of the NPAC SMS by swamping it with spurious messages

7.9.2 Security Services

R7-89 Authentication

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support Authentication (at association setup).

R7-90 Data Origin Authentication

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support data origin authentication for each incoming message.

R7-91.1 Detection of Message Replay

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support detection of replay.

R7-91.2 Deletion of a Message

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support detection of message deletion.

R7-91.3 Modification of a Message

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support detection of message modification.

R7-91.4 Delay of a Message

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support detection of message delay.

R7-92 Non-repudiation of Origin

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall support non-repudiation of origin.

R7-93 Access Control

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall allow only authorized parties (i.e., carriers serving a given customer) to cause changes in the NPAC SMS database.

7.9.3 Security Mechanisms

This section outlines the requirements to specify security mechanisms.

7.9.3.1 Encryption

R7-94.1 Public Key Crypto System (PKCS)

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall use a public key crypto system (PKCS) to provide digital signatures. Since there is no requirement for confidentiality service there is no need for any additional encryption algorithms.

R7-94.2 Digital Signature Algorithms

NPAC SMS shall support one of the digital signature algorithms listed in the OIW Stable Implementation Agreement, Part 12, 1995.

R7-95 RSA Encryption Modulus Size

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall require the size of the modulus of each key to be at least 600 bits for RSA encryption.

7.9.3.2 Authentication

R7-96 Digital Signature Algorithm

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall apply the digital signature algorithm to the fields specified below without any separators between those fields or any other additional characters.

- The unique identity of the sender
- The Generalized Time, corresponding to the issuance of the message
- A sequence number
- A key identifier
- Key list ID

R7-97 Authenticator Contents

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall provide authentication consisting of the following:

- The unique identity of the sender
- The Generalized Time, corresponding to the issuance of the message
- A sequence number
- A key identifier
- The digital signature of the sender's identity, Generalized Time and sequence number listed above
- Key list ID

R7-98 Authenticator in Access Control Field

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall convey the authenticator in the CMIP access control field.

7.9.3.3 Data Origin Authentication

R7-99.1 Subsequent Messages Contain Access Control Field

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall ensure that every subsequent CMIP message that contains the access control field carries the authenticator.

R7-99.2 Separate Counter for Association Sequence Numbers

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall verify that each party maintains a separate sequence number counter for each association it uses to send messages.

R7-99.3 Increment Sequence Numbers

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall verify that every time the authenticator is used the value of the sequence number will be incremented by one.

7.9.3.4 Integrity and Non-repudiation

R7-100.1 Security Field

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall ensure that all the notifications defined for the number portability application contain a security field.

R7-100.2 Security Field Syntax

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall ensure that the syntax of the security field used for the notification corresponds to the authenticator.

R7-101.1

DELETE

R7-101.2

(Duplicate - refer to R7-91.1)

R7-101.3

(Duplicate - refer to R7-91.2)

R7-101.4

(Duplicate - refer to R7-91.3)

R7-101.5

(Duplicate - refer to R7-91.4)

R7-102 Notifications in Confirmed Mode

NPAC SMS shall ensure that all the notifications are sent in the confirmed mode.

R7-103

MISSING in RFP

7.9.3.5 Access Control

R7-104 Responsible for Access Control

NPAC SMS shall be responsible for access control on the SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface.

R7-105.1

(Duplicate - refer to R7-97 and R7-98)

R7-105.2 Generalized Time

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall ensure that external messages received have a generalized time in the access control information within 5 minutes of the NPAC SMS system clock.

7.9.3.6 Audit Trail

R7-106 Log Contents

SOA to NPAC SMS interface and the NPAC SMS to Local SMS interface shall keep a log of all of the following:

- Incoming messages that result in the setup or termination of associations
- All invalid messages (invalid signature, sequence number out of order, Generalized Time out of scope, sender not authorized for the implied request)
- All incoming messages that may cause changes to the NPAC SMS database

7.9.3.7 Key Exchange

R7-107.1 Lists of Keys

NPAC SMS shall ensure that during a security key exchange, each party provide the other with a list of keys.

R7-107.2 Keys in Electronic Form

NPAC SMS shall provide the list of keys in a secure electronic form.

R7-107.3 Paper copy of MD5 Hashes of the Keys

The originator of the list of keys shall also provide the receiver with signed (in ink) paper copy of the MD5 hashes of the keys in the list.

R7-107.4 Key List Exchange

NPAC SMS shall support exchange of the list of keys in person or remotely.

R7-107.5 Remote Key List Exchange

NPAC SMS shall convey the lists via two different channels, diskette sent via certified mail, and a file sent via Email or FTP using encryption mechanisms if the keys are exchanged remotely.

R7-108.1 Remote Reception Acknowledgment

NPAC SMS shall support the Service Providers' acknowledgment via 2 secure electronic forms, Email or FTP using encryption mechanisms.

R7-108.2 Acknowledgment Contents

NPAC SMS shall support the acknowledgment consisting of the MD5 hash of each one of the keys in the list.

R7-108.3 Phone Confirmation

The recipient shall call the sender by phone for further confirmation and provide the sender with the MD5 hash of the whole list.

R7-109.1 Periodic Paper List of Public Keys NPAC Uses

NPAC SMS shall generate a paper list to each Service Provider of the MD5 hashes of all the public keys used by a Service Provider once a month.

R7-109.2 Acknowledgment of Paper List of Public Keys

NPAC SMS shall verify the identity of the Service Provider to whom the MD5 hashes of the public keys was sent.

R7-110.1 List Encryption Keys

NPAC SMS shall provide each Service Provider with a numbered list of encryption keys, numbered from 1 to 1000.

R7-110.2

(Duplicate - refer to R7-107.2)

R7-110.3 List Encryption Keys

NPAC SMS shall ensure unique numbering of the keys.

R7-111.1 New Encryption Key Can Be Chosen

NPAC SMS shall allow a new encryption key to be chosen with every message that contains a key identifier.

R7-111.2 Keys Not Reused

NPAC SMS shall reject messages that use a key whose usage has stopped.

R7-111.3 Compromised Keys

NPAC SMS shall allow authorized NPAC SMS personnel to initiate a new key for messages.

R7-111.4 Key Change Once Per Year

NPAC SMS shall change the key used between the NPAC SMS and Service Provider after one year of usage.

R7-111.5 Key Size Increase Per Year

NPAC SMS shall allow NPAC SMS personnel to change key sizes for Service Providers as needed to ensure secure communications between the NPAC SMS and the Service Providers.

R7-111.6 Per Service Provider Application Basis

NPAC SMS shall expect new key initiation to be requested on a per Service Provider application basis.

RR7-1 Load Key List

NPAC SMS shall be able to load a new key list in 15 minutes or less.

This change order should be sized as a point release as early as possible during or prior tp turn-up testing with the service providers.

RN7-1 Authenticator Contents - Individual System Clock Accuracy

NPAC SMS shall be responsible for ensuring that the system clock is accurate to within two minutes of GMT.

RN7-2 Authenticator Contents - Zero Sequence Number

A sequence number equal to zero shall be required for association request and association response messages.

RR7-2 Modifying User Name

NPAC SMS shall provide a mechanism for authorized NPAC personnel to change a user name in the NPAC SMS.

8. Audit Administration

8.1 Overview

An audit function will be necessary for troubleshooting a customer problem and also as a maintenance process to ensure data integrity across the entire LNP network. Audit will be concerned with the process of comparing the NPAC view of the LNP network with one or more of the Service Provider's view of its network. In the case of "on demand" audits, audits may be initiated by any Service Provider who has reason to believe a problem may exist in another Service Provider's network. Such audits are executed via queries to the appropriate Service Provider's network, and corrected via downloads to those same networks. Requirements pertaining to these requirements are given in Sections 8.2 through 8.6.

With audits, two different scenarios are supported, one designed to "sync up" the information contained in the various Local SMS databases with the content of the NPAC SMS database, the other for the NPAC to perform random integrity checks of its own database.

The local SMS will be responsible for comparing database extracts written to an FTP site by the NPAC SMS with its own version of that same data. Note that the Service Provider network may contain several network nodes designated for local number portability and may also choose to keep its own copy in its respective SMS. In the second scenario, the NPAC SMS will select a random sample of active Subscription Versions from its own database, then compare those samples to the representation of that same data in the various Local SMS databases. Requirements pertaining to periodic audits are given in Section 8.7.

A8-1 Service Provider Audits Issued Immediately

NPAC SMS will process audit requests from service providers immediately.

8.2 Service Provider User Functionality

R8-1 Service Providers Audit Request - Single TN

NPAC SMS shall receive an audit request on a single telephone number from the Service Providers.

R8-2.1 Service Providers Audit Request - Range of TNs

NPAC SMS shall receive an audit request for a range of telephone numbers from the Service Providers.

R8-2.2

DELETE

R8-3 Service Providers Specify Audit Scope

NPAC SMS shall allow Service Providers to specify the scope of an audit by specifying one or more of the following parameters:

- Specific Service provider network or ALL Service Providers networks
- Full audit for all LNP attributes or a partial audit where the Service Provider can specify one or more of the following LNP attributes:
  - LIDB data
  - CLASS data
  - LRN data
  - CNAM data
  - ISVM data

  Default: Full audit

8.3 NPAC User Functionality

R8-4 NPAC Personnel Audit Request - Single TN

NPAC SMS shall allow NPAC personnel to issue an audit request on a single telephone number.

R8-5.1 NPAC Personnel Audit Request - Range of TNs

NPAC SMS shall allow NPAC personnel to issue an audit request for a range of telephone numbers.

R8-5.2

DELETE

R8-6.1 Specify an Immediate Audit Request

NPAC SMS shall provide NPAC personnel and users of the SOA to NPAC SMS interface the capability to issue an audit request to be executed immediately.

R8-6.2

DELETE

R8-7.1

DELETE

R8-7.2

DELETE

R8-7.3

DELETE

R8-8

DELETE

R8-9 NPAC Personnel Specify Audit Scope

NPAC SMS shall allow NPAC SMS Personnel to specify the scope of an audit by specifying one or more of the following parameters:

- Specific Service Provider network or ALL Service Providers networks.
- Full audit for all LNP attributes or a partial audit where the Service Provider can specify one or more of the following LNP attributes:
  - LIDB data
  - CLASS data
  - LRN data
  - CNAM data
  - ISVM data

  Default: Full audit

Specify an activation Date/Time stamp range, i.e., only audit records activated between a specific time window.

R8-10 NPAC Personnel Status of Audit Request

NPAC SMS shall allow NPAC personnel to obtain the final results of an audit request.

R8-11 Audit Progress Indicators

NPAC SMS shall indicate the progress of an audit as the percentage of records audited, when supplying the status of an audit request.

R8-12 NPAC Personnel Cancel of an Audit

NPAC SMS shall allow NPAC personnel to cancel an audit request.

R8-13

DELETE

R8-14.1

DELETE

R8-14.2

DELETE

8.4 System Functionality

R8-15.1 NPAC Personnel View of ALL Audit Requests

NPAC SMS shall allow NPAC Personnel to view ALL audit requests including requests issued by the Service Providers.

R8-15.2 Mechanized SOA Interface Obtain Audit Requests

NPAC SMS shall allow the mechanized SOA interface to obtain all audit requests issued from that particular mechanized SOA interface.

R8-15.3 Send Audit Results to Originating SOA

NPAC SMS shall send audit results to the originating SOA.

R8-16.1 Flow of Audit Execution

NPAC SMS shall send the query resulting from the audit request to the local Service Providers' networks that are accepting Subscription Version data downloads for the given NPA-NXX via the NPAC SMS to Local SMS interface, as described in the NPAC SMS Interoperable Interface Specification.

R8-16.2

DELETE

R8-16.3

DELETE

R8-16.4

DELETE

R8-17.1 Compare NPAC SMS Subscription Versions to Service Provider Subscription Versions

NPAC SMS shall conduct a comparison of the Subscription Versions belonging to the Service Provider to its own Subscription Versions.

R8-17.2 Add TNs to Service Provider Subscription Versions

NPAC SMS shall, following the comparison of its own Subscription Versions to the Service Provider's Subscription Versions, add any TN found to be absent back into the Service Provider's Subscription Version database.

R8-17.3 Modify Erroneous TNs

NPAC SMS shall, following the comparison of its own Subscription Versions to the Service Provider's Subscription Versions, modify any TN found to be in error.

R8-17.4 Delete Discrepant TNs from Service Provider Subscription Versions

NPAC SMS shall, following the comparison of its own Subscription Versions to the Service Provider's Subscription Versions, delete any discrepant TNs from the Service Provider's Subscription Version database.

R8-18

(Duplicate - refer to R8-7.3)

R8-19 Record Audit Results in an Audit Log

NPAC SMS shall record all audit results in an audit log.

8.5 Audit Report Management

R8-20 Service Providers Audit Retrieval

NPAC SMS shall allow NPAC personnel and Service Provider personnel to retrieve an audit report for a specific audit request.

R8-21.1 Generate an Audit Report

NPAC SMS shall be capable of generating an audit report for each audit request that has been requested.

R8-21.2 Audit Report Contents

NPAC SMS shall generate an audit report containing the following information:

- Audit request parameters which identified the scope of the audit.
- Date and Time of Audit.
- Progress indication.
- Service Provider network which contains database conflict.

A difference indicator which indicates one of the following:

- Mismatch between the NPAC SMS and local SMS
- Record missing in local SMS
- An audit failure
- No discrepancies found

R8-22 NPAC Personnel Generate and View an Audit Report

NPAC SMS shall allow NPAC and Service Provider personnel to generate and view an audit report on-line.

R8-23.1 NPAC Personnel View an In-progress Audit Report

NPAC SMS shall allow NPAC personnel to view an audit report while the audit is in progress so the current audit results can be viewed on-line up to this point.

R8-23.2 Service Providers View Results of Audits They Have Requested

NPAC SMS shall ensure that Service Providers can only view the results of those audits which they have requested.

R8-24

(Duplicate - refer to R9-2)

R8-25 NPAC Personnel Specify Time Audit Results Retained

NPAC SMS shall allow NPAC personnel to specify the length of time audit results will be retained in the audit log.

8.6 Additional Requirements

RX8-1 Valid Audit Statuses

NPAC SMS shall support the following valid audit statuses:

- In-progress
- Canceled
- Complete

8.7 Database Integrity Sampling

RR8-1 Random Sampling of Active Subscription Versions

NPAC SMS shall select a random sample of active Subscription Versions to query over the NPAC SMS to Local SMS interface to monitor NPAC SMS data integrity.

RR8-2.1 Data Integrity Sample Size - Tunable Parameter

NPAC SMS shall provide a Data Integrity Sample Size tunable parameter which is defined as the number of active Subscription Versions in the sample to monitor NPAC SMS data integrity.

RR8-2.2 Data Integrity Sample Size - Tunable Parameter Modification

NPAC SMS shall allow the NPAC SMS Administrator to modify the Data Integrity Sample Size tunable parameter.

RR8-2.3 Data Integrity Sample Size - Tunable Parameter Default

NPAC SMS shall default the Data Integrity Sample Size tunable parameter to 1000.

RR8-3.1 Data Integrity Frequency - Tunable Parameter

NPAC SMS shall provide a Data Integrity Frequency tunable parameter which is defined as the frequency in days that the data integrity sampling is performed.

RR8-3.2 Data Integrity Frequency - Tunable Parameter Modification

NPAC SMS shall allow the NPAC SMS Administrator to modify the Data Integrity Frequency tunable parameter.

RR8-3.3 Data Integrity Frequency - Tunable Parameter Default

NPAC SMS shall default the Data Integrity Frequency tunable parameter to seven days. The allowable range is between one and ninety (1-90) days.

9. Reports

9.1 Overview

The NPAC SMS must support scheduled and ad hoc report generation for selectable reports. The report generation service shall create output report files according to specified format definitions, and distribute reports to output devices as requested. A report distribution service is used to distribute report files to selected output devices. Authorized NPAC personnel can request reports from active database, history logs, error logs, traffic measurements, usage measurements, and performance reports.

9.2 User Functionality

R9-1 NPAC Personnel Report Selection

NPAC SMS shall allow NPAC personnel using the NPAC Administrative Interface to select the type of report required.

R9-2 NPAC Personnel Selection of Output Destination

NPAC SMS shall allow NPAC personnel using the NPAC Administrative Interface to select the predefined report output destination. Destinations are printer, file system, email, display or FAX.

R9-3 NPAC Personnel Re-print of Reports

NPAC SMS shall allow NPAC personnel using the NPAC Administrative Interface to re-print reports from previously saved report outputs.

R9-4 NPAC Personnel Create Customized Reports

NPAC SMS shall allow NPAC personnel to create customized reports through an ad-hoc facility.

R9-5 NPAC Personnel Define Scope and Filtering

NPAC SMS shall allow NPAC personnel to define scope and filtering for items to be included in the customized reports.

R9-6 Service Providers Receive Reports on Their Activities

NPAC SMS shall allow Service Provider personnel to receive reports on information related to their activities.

R9-7

DELETE

RX9-1 Service and Network Data Reports

NPAC SMS shall support the following service and network data reports for NPAC personnel using the NPAC Administrative Interface and Service Provider personnel using the NPAC SOA Low-tech Interface:

1. NPAC Service Tunable Parameters Report
2. List of Service Provider's LRNs
3. Open NPA-NXXs List

RX9-2 Service Provider Reports

NPAC SMS shall support the following Service Provider reports for NPAC personnel using the NPAC Administrative Interface and Service Provider personnel using the NPAC SOA Low-tech Interface:

4. Service Provider Profile (Service Provider's own data only)
5. Service Provider's Subscription List by Status (Service Provider's own data only)

RX9-3 Subscription Data Reports

NPAC SMS shall support the following subscription data reports for NPAC personnel using the NPAC Administrative Interface and Service Provider personnel using the NPAC SOA Low-tech Interface:

6. Subscriptions Listed by Status
7. Subscriptions Listed by Service Provider by Status

RX9-4 System Reports

NPAC SMS shall support the following system reports for NPAC system administration personnel using the NPAC Administrative Interface:

8. Overall CPU System Utilization
9. Storage Utilization
10. NPAC SMS Application Performance (SOA/LSMS Downloads per Second)
11. NPAC SMS Application Performance (SOA/LSMS Subscription Activation Time)
12. NPAC SMS-SOA Link Utilization
13. NPAC SMS-LSMS Link Utilization
14. NPAC SMS Application Performance (SOA/LSMS Response Time)
15. NPAC SMS Application Performance (Interface Transaction Rate)
16. NPAC SMS Application Performance (Provider SMS Database Sampling)

RX9-5 Security Reports

NPAC SMS shall support the following security reports for NPAC security administration personnel using the NPAC Administrative Interface:

17. Access Privileges Matrix
18. Authorized Users List
19. Security Log
20. Invalid Access Attempts
21. Encryption Keys List

RX9-6 Log File Reports

NPAC SMS shall support the following log file reports for NPAC personnel using the NPAC Administrative Interface:

22. History Report
23. Error Report
24. Service Provider Notification Report
25. Subscription Transaction Report
26. Service Provider Administration Report
27. Subscription Administration Report

RX9-7 Audit Reports

NPAC SMS shall support an Audit Results Report.

RX9-8 Regularly Scheduled Reports

NPAC SMS shall support the generation of regularly scheduled standard or ad hoc reports, to be provided at the request of a Service Provider.

RR9-1 Data Integrity Report

NPAC SMS shall generate an NPAC SMS data integrity report.

9.3 System Functionality

R9-8

(Duplicate - refer to R9-2)